IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this paper is being transmitted electronically to the US Patent Office on 17 September 2007.

Rosalie A. Centeno

Rosalie A. Centeno

Appl. No.	:	10/633,918
Applicant	:	Hamdy Soliman
Filed	:	04 August 2003
For	:	Computer System Security Via Dynamic Encryption
TC/A.U.	:	2131
Examiner	:	Jenise E. Jackson

Customer No: 30996

Board of Patent Appeals and Interference
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

MAIL STOP: APPEALS

Sir:

Appellant hereby appeals to the Board of Patent Appeals and Interferences from the decision dated April 17, 2007 of the Examiner finally rejecting claims 1 – 20.

1. According to the requirements of CFR 1.192, appellant herewith encloses an Appeal Brief.

2. The fee of $250.00 is enclosed in payment for filing such Appeal Brief. Applicant claims small entity status (37 CFR 1.27).

3. Appellant does not wish to arrange an oral hearing for this appeal.

If the amount enclosed should be insufficient, please charge the remainder to Deposit Account No. 02-1653.

Respectfully Submitted,

Robert W. Becker

Robert W. Becker, Reg. No. 26,255
for applicant

ROBERT W. BECKER & ASSOCIATES
707 State Hwy 333, Ste. B
Tijeras, New Mexico 87059-7507

Telephone: 505 286 3511
Telefax: 505 286 3524

RWB:rac

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

I hereby certify that this paper is being transmitted electronically to the US Patent Office on 17 September 2007.

Rosalie A. Centeno

Rosalie A. Centeno

In re Application of:	Hamdy Soliman
For:	Computer System Security Via Dynamic Encryption
Filing Date:	August 4, 2003
Application Number:	10/633,918
Attorney Docket Number:	NMTECH13.CIP2
Group Art Unit:	2131
Examiner:	Jenise E. Jackson

APPELLANT'S APPEAL BRIEF

To: Mail Stop APPEAL BRIEFS-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Appellant respectfully submits this Appeal Brief with the Board of Patent Appeals and Interferences in response to the Examiner's final rejection. Applicant hereby requests the Board to overrule the Examiner's rejections and to allow the rejected claims in the application.

TABLE OF CONTENTS

(1) REAL PARTY IN INTEREST

The real party in interest is the Assignee, New Mexico Technical Research Foundation.

(2) RELATED APPEALS AND INTEFERENCES

No other appeals or interferences will directly affect, be directly affected by, or have a bearing on the Board's decision in this appeal.

(3) STATUS OF CLAIMS

Claims 1-20 are pending in the application.
Claims 1-20 have been finally rejected and are being appealed.
The appealed claims are set forth in Section (8).

(4) STATUS OF AMENDMENTS

None.

(5) SUMMARY OF THE CLAIMED SUBJECT MATTER

A. The method of independent claim 1 includes method of providing a secure data stream between system nodes. The method of claim 1 includes a first step that recites providing a data record block including a plurality of data records encrypted within a predetermined time interval. Support for the first step of claim 1 can be found in the specification at page 5, line 23 to page 6, line 17, page 25, lines 21-27, page 26, lines 3-14, page 27, lines 17-26 and Figures 11, 13a and 13b. A second step of the method of claim 1 recites providing a previous encryption key, also referred to as a dynamic session key (DSK). The second step of the method of claim 1 is described in the specification at page 5, line 23 to page 6, line 17, page 26, lines 3-14, page 27,

lines 17-26 and Figures 11, 13a, and 13b. In a third step of the method of claim 1, the method recites selecting an old data record from the plurality of data records, support for which is found in the specification at page 5, line 23 to page 6, line 17, page 25, lines 21-27, page 26, lines 3-14, page 27, lines 17-26 and Figures 11, 13a and 13b. The fourth step of the method of claim 1 recites regenerating a new encryption key at a user node as a function of the previous encryption key and the old data record. The fourth step of the method of claim 1 is described in the specification at page 6, lines 3- 17, page 26, lines 3-14, page 27, lines 17-26 and Figures 8, 9, 11, 13a, and 13b.

B. The system of independent claim 19 includes a system for providing a secure data stream between a source programmable apparatus and a destination programmable apparatus. The system includes a first element including a source programmable apparatus. A source programmable apparatus is also defined in the specification as a node or one or more computers that are in electrical communication such as via a computer network. See specification at page 10, lines 15-20. The source programmable apparatus can also include computer-readable memory for providing storage for the data, performing dynamic key changing and to carry out other necessary processes within the computer. See specification at page 10, lines 21-25. A second element of the system of claim 19 includes a data stream created by said source programmable apparatus, which is described in the specification at page 10, line 21. Element three of the system of claim 19 includes means for encrypting a data record of said data stream with a previous encryption key forming an encrypted data record. The means for encrypting can include for example computer-readable means such as software and the necessary related hardware as described in the specification at page 11, lines 1-2. The function of encrypting is described above with reference to claim 1, and is further detailed in the specification at page 5, line 23 to page 6, line 17, page 25, lines 21-27, page 26, lines 3-14, page 27, lines 17-26 and Figures 11, 13a and 13b. A fourth element of the system of claim 19 includes means for regenerating a new encryption key as a function of the previous encryption key and an old data record. As noted above, the means for regenerating can include for

example computer-readable means such as software and the necessary related hardware as described in the specification at page 11, lines 1-2. The function of regenerating a new encryption key is noted above with reference to claim 1, and described in detail in the specification at at page 6, lines 3- 17, page 26, lines 3-14, page 27, lines 17-26 and Figures 8, 9, 11, 13a, and 13b.

(6) GROUNDS FOR REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-20 have been finally rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,292,896 to Guski et al.

(7) ARGUMENTS

A. Claims 1-20 are not anticipated under 35 U.S.C. §102(b) over U.S. Patent No. 6,292,896 to Guski et al.

The Examiner finally rejected independent claims 1 and 19 and dependent claims 2-18 and 20 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,292,896 to Guski et al. ("Guski"), a rejection that Appellant respectfully traverses because Guski does not disclose each and every limitation of the claims as presented. Accordingly, Appellant respectfully urges the Board to overrule the rejection of independent claims 1 and 19 and dependent claims 2 -18.

35 U.S.C. §102 (b), cited by the Examiner as the basis for rejection of Claims 1-20, provides:

"A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States...."

Appellant respectfully submits that Guski does not anticipate claims at least claims 1 and 19 because the Guski does not disclose each and every element claimed by the Appellant. Guski does not satisfy the "all-elements" rule of MPEP §2131, which provides:

> A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference...The identical invention must be shown in as complete detail as contained in the claim...[and] the elements must be arranged as required in the claim. (Emphasis added)

Claims 1 and 19 are allowable for the simple reason that Guski at least fails to disclose that a new encryption key is regenerated at the user node as a function of the previous encryption key and the old data record, as recited in claims 1 and 19 and incorporated by reference into claims 2-18 and 20.

Claim 1 recites in part:

> "[...]providing a previous encryption key;
>
> selecting an old data record from the plurality of data records; and
>
> regenerating a new encryption key at a user node as a function of the previous encryption key and the old data record."

With respect to claim 1, the Examiner referred to Guski at col. 9, lines 11-34, 44-54, for the proposition that it allegedly teaches or discloses "selecting encrypted data; and regenerating a new encryption key at a node with an encryption key and selected encrypted data." As shown above, claim 1 recites that the new encryption key is regenerated at the user node as a function of the previous encryption key and the old data record.

The cited passages of Guski teach a key weakening function, which is a method for deriving another a weakened session key (KS) from a strong key (K'). As noted by Guski, this method involves passing the original value K' through a plurality of functions, including a non-key-bit set function, a one-way function, a key-bit-select function and a randomized key-select function. The first three functions create intermediate keys from the original value K', and the fourth function, operating on the third intermediate value, creates the weakened session key KS. Guski at col. 9, lines 5-65.

However, Guski does not teach or disclose regenerating a new encryption key as a function of a previous encryption key and an old data record, as recited in claim 1. On the contrary, Guski specifically teaches the use of a multitude of functions operating in a linear fashion on a single input value, i.e. the original value K', the first intermediate key, the second intermediate key, and the third intermediate key. As Guski does not teach or disclose each and

every limitation of claim 1, Appellant respectfully submits that claim 1, and its dependents 2-18, are in condition for allowance.

With respect to claim 19, the Examiner cited the same passages from Guski as allegedly teaching "means for regenerating a new encryption key as a function of the previous encryption key and an old data record." To the extent that this recitation from claim 19 is similar to claim 1, Appellant respectfully submits that the arguments provided above are equally applicable herein. In particular, as noted above, Guski teaches a single input value K' for producing the weakened session key KS. In contrast, claim 19 recites "means for regenerating a new encryption key as a function of the previous encryption key and an old data record." As Guski does not teach or disclose using an old data record as an input into the key-weakening steps recited therein, Appellant respectfully submits that claim 19 and its dependent claim 20 are also in condition for allowance.

In the final rejection, the Examiner provided a further citation of Guski that allegedly discloses the step and/or means for "regenerating a new encryption key as a function of the previous encryption key and an old data record." In particular, the Examiner cited Guski at Col. 8, lines 59-67 to Col. 9, lines 1-4, in support of this proposition. However, the cited passage reads as follows:

> "If the reverse translation procedure 602 determines that the received password 310 does not correspond to a legal password (step 704), then the password evaluator 312 denies access (step 706) without further processing, since the received password represents either an attempt to break into the system or a corruption of data.
>
> "If the received password 310 does correspond to a legal password, then the password evaluator 312 determines whether the received password is identical to any valid password received over a predefined time interval (step 708); the interval is 10 minutes in the disclosed embodiment, but may be more or less if desired."

Appellant respectfully submits that the cited passage does not teach or disclose any means or method of regenerating a new encryption key as a function of the previous encryption key and an old data record.

The Examiner further alleges that the step and/or means for "regenerating a new encryption key as a function of the previous encryption key and an old data record" is disclosed

in Guski at col. 12, lines 17-27, lines 29-47. Lines 17-47 of column 12 are reproduced below:

> "Session key 319 (KS) is generated in the same manner at the authenticating node 104 at step 1404 as the identical session key 311 was at the requesting node 102 at step 1104, with the time value T being the regenerated value 626 obtained from the received password 310. Referring to FIG. 6, the authenticating node copy of the signon key K (314) provides the key input to a DES encryption function 630 (invoked only for session key generation and not for password evaluation) to produce a output value K' (632) identical to the value K' (428) generated at the requesting node 102.
>
> "The input 634 to DES encryption function 630 is identical to the input 430 to the DES encryption function 426 at the requesting node 102 and is obtained in a similar manner by concatenating the regenerated and validated time/date value T (626) with the right half D2P1 (617) of the second DES encryption product D2P (616). Values T and D2P1 are generated anew in response to the session key request by repeating the transformations 606-624 (but not the time comparison 628) previously performed for the signon request from target application 318. (Alternatively, values T and D2P1 may be saved from the previous handling of the signon request.) Value K' is passed through a key weakening function 636 identical to key weakening function 432, and invoked only for session key generation and not for password evaluation, to produce the authenticating node copy of session key KS (638) as an output."

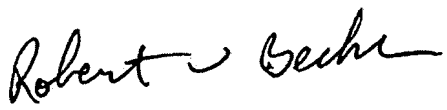
Again, Appellant is unable to find any reference, teaching or disclosure of the noted limitation in the passage reproduced above. On the contrary, the cited passage deals with the generation and authentication of session keys, which are clearly not the same as the data records and encryption keys described and claimed in the present invention. By way of comparision, the present invention is motivated in part by the weaknesses inherent in the current session key systems, especially those that employ symmetric encryption systems such as DES. See Description, page 2, line 16 to page 3, line 2.

Appellant respectfully submits that the foregoing passage fails to teach or disclose the step and/or means of "regenerating a new encryption key as a function of the previous encryption key and an old data record." Therefore, in accordance with the all-elements rule noted above, Appellant notes that at least one step of independent claim 1 and at least one element of independent claim 19 is not anticipated by Guski. As each of the remaining claims depend, either directly or indirectly, from claim 1 or 19, Appellant hereby requests that all of the pending claims be allowed as currently presented.

Conclusion

In view of the foregoing, Appellant respectfully requests that the Board of Patent Appeals and Interferences overrule the Final Rejection of claims 1-20 over the cited art, and hold that Appellants' claims 1-20 are allowable.

Respectfully Submitted,



Robert W. Becker, Reg. No. 26,255
Attorney for Applicant

Robert W. Becker & Associates
707 Highway 333 East, Suite B
Tijeras, NM 87059

Telephone: (505) 286-3511
Facsimile: (505) 286-3524

RWB/rac

(8) CLAIMS APPENDIX

Listing of Claims as Last Amended

1. A method of providing a secure data stream between system nodes, the method comprising:

providing a data record block including a plurality of data records encrypted within a predetermined time interval;

providing a previous encryption key;

selecting an old data record from the plurality of data records; and

regenerating a new encryption key at a user node as a function of the previous encryption key and the old data record.

2. The method of claim 1 wherein the step of selecting the old data record comprises selecting the old data record using a byte from the previous encryption key as a seed of random generation.

3. The method of claim 1 wherein the step of regenerating the new encryption key comprises regenerating a new encryption key by performing a logic operation on the previous encryption key and the old data record.

4. The method of claim 3 wherein the step of regenerating the new encryption key by performing a logic operation comprises regenerating the new encryption key by performing an XOR logic operation on the previous encryption key and the old data record.

5. The method of claim 3 wherein the step of regenerating the new encryption key by performing a logic operation comprises performing the logic operation on the previous encryption key and the old data record to form an expanded key.

6. The method of claim 5 further comprising the step of selecting bytes from the expanded key to generate the new encryption key.

7. The method of claim 6 wherein the step of selecting bytes from the expanded key to generate the new encryption key comprises randomly selecting bytes from the expanded key to generate the new encryption key.

8. The method of claim 7 wherein the step of randomly selecting bytes from the expanded key to generate the new encryption key comprises randomly selecting bytes from the expanded key using a byte from the previous encryption key as a seed of random generation.

9. The method of claim 1 further comprising the step of encrypting a new data record with the new encryption key forming a new encrypted data record.

10. The method of claim 9 wherein the step of encrypting the new data record with the new encryption key comprises performing a logic operation on the new data record and the new encryption key.

11. The method of claim 10 wherein the step of performing a logic operation on the new data record and the new encryption key comprises performing an XOR operation on the new data record and the new encryption key.

12. The method of claim 10 wherein the step of performing a logic operation on the new data record and the new encryption key comprises forming a cipher.

13. The method of claim 12 further comprising the step of permuting portions of the cipher to form another cipher.

14. The method of claim 9 further comprising the step of transmitting the new encrypted data record over a data stream.

15. The method of claim 14 further comprising the step of receiving the new encrypted data record at a destination node.

16. The method of claim 15 further comprising the step of decrypting the new encrypted data record at the destination node.

17. The method of claim 16 wherein the step of decrypting the new encrypted data record comprises decrypting the new encrypted data record with a previous decryption key forming a new decrypted data record.

18. The method of claim 17 further comprising the step of regenerating a new decryption key as a function of the new decrypted data record and the previous decryption key.

19. A system for providing a secure data stream between a source programmable apparatus and a destination programmable apparatus, the system comprising:

a source programmable apparatus;

a data stream created by said source programmable apparatus;

means for encrypting a data record of said data stream with a previous encryption key forming an encrypted data record; and

means for regenerating a new encryption key as a function of the previous encryption key and an old data record.

20. The system of claim 19 further comprising:

a destination programmable apparatus in communication with said source programmable apparatus;

means for transmitting the encrypted data record to said destination programmable apparatus;

means for decrypting said the encrypted data record received at said destination programmable apparatus with a previous decryption key forming a decrypted data record; and

means for regenerating a new decryption key as a function of the previous decryption key and the decrypted data record.

(9) EVIDENCE APPENDIX

None.

(10) RELATED PROCEEDINGS APPENDIX

None.